DEPAUW UNIVERSITY
ELECTRONIC COMMUNICATIONS AND ACCEPTABLE USE POLICY
(01-07-2006)

I. INTRODUCTION

The University has adopted this Policy in part to: encourage employee and student productivity; maintain the integrity and security of its network and computing resources and electronic communication systems; preserve its academic and business interests; and protect confidential information. This Policy cannot and does not provide rules and requirements to address every possible situation that may arise. However, it does provide certain minimum standards and requirements with respect to electronic communication issues. The University reserves the right to change, revise or add to this Policy at any time with such notice as it deems appropriate.

Under its Intellectual Property policy, the University has granted to faculty members the intellectual property rights to materials they have authored (articles, books, software, manuscripts, syllabi and course materials) and the results of their research. Faculty members may be required to provide copies of course materials or research protocols if needed for personnel reviews, program reviews, or campus disciplinary proceedings, including the enforcement of this or other policies. All other aspects of the University's electronic communication facilities, including all equipment and data, messages, or other information transmitted, stored or maintained on or in such facilities, are and remain at all times the property of the University, unless otherwise expressly noted in a written confirmation signed by an authorized University official. However, such ownership shall not include any such information that is in violation of any University policy, including, but not limited to, this Policy.

DePauw University recognizes and honors the importance of academic freedom, and the provisions of the Policy will be enforced with respect to the teaching and research mission of the University.

II. POLICIES

A. Permissible Uses of Electronic Communication Facilities

1. Electronic communication facilities are intended to be used primarily for official University business, including employee and student academic pursuits, and employee administrative, personnel and/or business matters. However, reasonable use of University-owned or operated electronic communication facilities for non-commercial personal purposes is permitted if it does not entail a direct cost to the University, interfere with the completion of job responsibilities, impede network operations, or violate University policies, including, but not limited to this Policy. Should users make use of the electronic communication facilities to transmit personal messages, such messages shall not be treated with a higher standard of privacy than any other electronic communication. The University reserves the right to place additional restrictions on the personal use of its electronic communication facilities if necessary to conserve network resources for University purposes. Further, those using the University's electronic communication facilities must use such facilities in a responsible and lawful manner. Unlawful use of electronic communication facilities or use of such facilities which violates any University policy, including this policy, by any user, as determined solely by University officials, will be cause for the University to deny such user further access to such facilities and may be cause for other University disciplinary action, up to and including termination from employment or expulsion.

2. Consistent with this Policy, users may use the electronic communication facilities to initiate or receive electronic communication. lpeir3usTc 0 Tw ination from eUr Univwiesilmess0 eiversh facildp

f. Electronic communication facilities shall not be used in violation of University policies or local, state or federal laws, rules or regulations.

g. Users shall not abuse or vandalize any electronic communication facilities. Users are to immediately report any observed or suspected instances of abuse or vandalizing of electronic communication facilities to University officials.

h. Users should relinquish public computing facilities that they are using if they are doing non-essential work when the computers are in heavy demand. Electronic communication facilities should not be monopolized.

3. Security/Breach of Security

a. Although the University uses various methods in an effort to secure its electronic communication facilities, the University cannot guarantee such security. Electronic communication and electronic communication facilities shall not be used to breach the electronic security of others. A breach of security includes, but is not limited to: any unauthorized attempt to compromise any electronic communication facility, including the use of network privileges, accounts, access codes, identifiers or passwords, or equipment; knowing and unauthorized interception, access, disclosure, disruption, damage, destruction or unauthorized alteration/modification of any electronic information, or electronic communication facilities, including software or hardware; and any unauthorized and intentional disruption or interference with others' use of electronic communication facilities.

b. Users of electronic communication facilities are responsible for protecting their personal account information and/or password. Any user holding a personal account and its password is, at all times, responsible for its use and all activity originating from that account or using that password. Any attempt to determine the passwords or personal account information of others is strictly prohibited.

C. Privacy

Although University email messages are encrypted by University systems as part of the regular transmission process, the University cannot guarantee the privacy of electronic communications, and users should not expect their use of electronic communication facilities will be private. Users who further encrypt an electronic communication must furnish the encryption key or software to the University upon request so that the University may fulfill its obligations under the provisions of this policy.

III. MONITORING AND DISCLOSURE

A. In General

The University reserves the right to monitor or disclose the content of any electronic communication sent, received or stored using electronic communication facilities. Monitoring, investigation, and examination of electronic content will only be conducted in connection with a specific event, such as the delivery of a warrant for search and seizure or other permissible events as listed in the Policy. Employees are not permitted to engage in the monitoring, investigation, or examination of electronic communication content without prior specific authorization of the Chief Information Officer as specifically permitted under the Policy. Employees do regularly monitor the performance of the University's computing resources, and the University reserves the right to install or update files on any University-owned computer to assure the performance or security of the campus computing environment. Use of the electronic communication facilities shall be deemed to constitute consent to allow the University to exercise its rights outlined in this Policy and agreement to abide by this Policy.

B. Monitoring and Disclosure

As the owner or operator of electronic communication facilities and a private institution of higher education, the University will monitor or disclose the content of the electronic communication of users only under the following circumstances:

1. A party to the communication consents; or

2. The communication is readily accessible to the public (examples include, but are not limited to, web pages, e-mails sent to a public mailing list, or a newsgroup post); or

3. The University has an administrative need to access an e-mail, voice mail or other electronic communication or electronic communication facilities (examples include routine maintenance, backup of data, monitoring of usage patterns, troubleshooting or investigation of an excessive use of network resources that adversely affects performance or protection of the University's rights or property); or

4. The University is furnished with reasonable information causing it to conduct a review or investigation of any electronic communication or the use of electronic communication facilities (examples include reports or evidence of hacking, identity theft, harassment, commercial card fraud). The University has sole discretion to conduct such a review or investigation under this Policy; or

5. The monitoring or disclosure occurs as a result of the University's obligations under local, state and/or federal laws, rules or regulations.

IV. RETENTION AND ARCHIVAL STORAGE OF ELECTRONIC COMMUNICATIONS

A. Policies

Records created or stored in digital format, including electronic communication, may be subject to state or federal laws or University record-keeping policies.

B. Employee Responsibilities

Employees are responsible for copying electronic communication for storage in departmental or office files as required by law or University policy.

1. The University does not maintain centralized or distributed archives of electronic communication sent or received over its electronic communication facilities. Backups made for maintenance or troubleshooting purposes are erased at regular intervals.

2. Staff should periodically store such copies in departmental or office files for subsequent review followed by either archival storage or destruction in accordance with general University record-keeping policies.

V. ACCEPTANCE OF ELECTRONIC SIGNATURES

A. In General

[User] understands and agrees that by clicking the "I ACKNOWLEDGE" button the [User] is electronically signing the Request for Release of Educational Records or is authorizing specific University action and that the electronic signature is [User]' s valid and binding signature for purposes of the

Educational Records and authorization. [User] understands that: (1) All representations, information and electronic signature(s) [User] provides have the same force and effect they would have if made in non-electronic form; (2) DePauw University can and will rely on the Request for Release of Educational Records; and, (3) [User] intends to be bound to and electronically sign the Request for Release of Educational Records or other authorization by clicking the "I ACKNOWLEDGE" button.

[User] further agrees that Indiana's version of the Uniform Electronic Transactions Act (the "Act") applies to the Request for Release of Educational Records, that the Request for Release of Educational Records is a

5. "Monitor" and “monitoring” mean to intercept, access, or inspect an electronic communication with the purpose of viewing the data contained therein. "Monitor" does not include automatic scanning of an electronic communication by network security and performance software such as a firewall, anti-virus, or packet shaper program.

6. "Employees" means any and all full- and part-time, temporary and regular University employees including, but not limited to faculty members, administrators, instructors, staff members, classified personnel and student employees who have been authorized to use the electronic communication facilities.

7. "Students" means any and all students who have paid a deposit or are currently enrolled in the University, as well as former students who have been authorized to use the electronic communication facilities.

8. “Guests” means any and all persons not directly connected to the University, but who have been authorized to use the electronic communication facilities.

9. "University authorization", "University authorized", or authorization from the "University", a "University official", or "University officials" means any written or oral express permission granted by one of the following University representatives: the